UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,783	09/27/2000	Joseph Andrew Mellmer	1909.2.74A	6748

1009 7590 08/06/2007

KING & SCHICKLI, PLLC
247 NORTH BROADWAY
LEXINGTON, KY 40507

EXAMINER	
WOO, ISAAC M	
ART UNIT	**PAPER NUMBER**
2166	

MAIL DATE	DELIVERY MODE
08/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

SP

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/670,783
Filing Date: September 27, 2000
Appellant(s): MELLMER ET AL.

Michael T. Sanderson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 12, 2007 appealing from the Office action mailed February 21, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

1. The rejection of claims 1, 3-58 and 90-101 under 35 U.S.C. § 102(e), as being anticipated by O'Flaherty et al (U.S. Patent No. 6,275,824).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. Patent No. 6,275,824	O'Flaherty et al	08-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. The rejection of claims 1, 3-58 and 90-101 under 35 U.S.C. § 102(e), as being anticipated by O'Flaherty et al (U.S. Patent No. 6,275,824).

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 3-58 and 90-101 are rejected under 35 U.S.C. 102(e) as being anticipated by O'Flaherty et al (U.S. Patent No. 6,275,824, hereinafter, "O'Flaherty").

With respect to claim 1, O'Flaherty teaches, database (i.e., 102, secure data warehouse in fig. 1, fig. 2, col. 4, lines 30-36, col. 5, lines 29-50) including a vault (i.e., 106, extended database in fig. 2, col. 4, lines 10-28), the vault for storing of multiple user objects for multiple users (i.e., 202, customer table in fig. 2), the vault having access rights granted to a system administrator for management of the user objects (i.e., 202, customer table in fig. 2), each of the user objects having a corresponding safe object (i.e., each profile object for personal identity information in customer table 202 in fig. 2, is restricted for accessing by such as, standard view, privileged view or anonymizing view, col. 7, lines 10-67 to col. 8, lines 1-61), the safe object containing multiple different profiles accessed (fig. 2, col. 7, lines 10-67 to col. 8, lines 1-61) and administered exclusively by a single one of the multiple users at the exclusion of the system administrator (i.e., user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63), each profile including digital identity information provided by the single one of the multiple users (i.e., user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63) and operable to be shared with other of the multiple users having other multiple different profiles accessible (i.e., user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63) and administered exclusively by the other of the multiple users the sharing occurring exclusively upon initiation by the single one of the multiple users, see (i.e., any user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63, col. 11, lines 7-67 to col. 12, lines 1-55).

With respect to claim 3, O'Flaherty teaches, safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles, see (col. 4, lines 30-67 to col. 5, lines 1-16)

With respect to claims 4-7, O'Flaherty teaches, safe object also contains at least one drop box object, one application object with settings for an application, one view object, one access object, see (fig. 2A-C, col. 7, lines 10-67 to col. 8, lines 1-67).

With respect to claims 8, O'Flaherty teaches, an identity server and a web server (col. 2, internet service).

With respect to claims 9, O'Flaherty teaches, the identity server communicate using encrypted user names, see (col. 4, lines 49-60).

With respect to claim 10, O'Flaherty teaches, web server and the identity server are secured by a firewall, see (col. 4, lines 49-60).

With respect to claim 11, O'Flaherty teaches, identity server appliance, see (col. 7, lines 10-67 to col. 8, lines 1-67).

With respect to claims 12-13, O'Flaherty teaches, a zero-byte, installed client, see (col. 4, lines 1-60).

With respect to claim 14, O'Flaherty discloses, system comprises a provider model for access to the database, see (col. 4, lines 49-60).

With respect to claim 15, O'Flaherty discloses, abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data, see (fig. 2A-C, col. 7, lines 10-65).

With respect to claim 16, O'Flaherty discloses, programmatic interface to identity items and operations that correspond generally to directory service objects, see (col. 12, lines 9-55).

With respect to claim 17, O'Flaherty discloses, database includes multiple safe objects contained in a vault object, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 18, O'Flaherty discloses, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 19, O'Flaherty discloses, Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 20, O'Flaherty discloses, digital business card application object having a corresponding profile object which includes digital identity information provided by the user, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 21, O'Flaherty discloses, one user to receive updated profile information of another user using a link to the database partitioned directory services database, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 22, O'Flaherty discloses, partitioned directory services database, see (fig. 2, col. 4, lines 18-33).

With respect to claim 23, O'Flaherty discloses, account creation service which creates a new account for a user based on a template, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 24, O'Flaherty discloses, administrative tool to manage and maintain safe objects, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 25, O'Flaherty discloses, schema management service which permits an administrator to at least view a directory service schema, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 26, O'Flaherty discloses, batch account creation service which creates several accounts at one time, see (fig. 3A-C, col. 10, lines 10-67 to col. 11, lines 65).

With respect to claim 27, O'Flaherty discloses, install service which permits one to install and configure an identity server, see (col. 4, lines 1-67).

With respect to claim 28, O'Flaherty discloses, backup and restore service which allows one to backup and restore at least one safe object, see (col. 4, lines 1-67).

With respect to claim 29, O'Flaherty discloses, safe advisor service which allows one to verify the integrity of a safe object, see (col. 4, lines 1-67).

With respect to claim 30, O'Flaherty discloses, legal recovery tool which recovers digital identity information for forensic use, data demoralization service which facilitates data transformation on database fields, see (col. 4, lines 1-67).

With respect to claims 31, O'Flaherty discloses, data denormalization service which facilitates data transformation on database fields, see (col. 4, lines 1-67).

With respect to claim 32, O'Flaherty discloses, rules service, see (col. 4, lines 1-67).

With respect to claim 33, O'Flaherty discloses, identity server to register interest in and be notified of changes in the database, see (col. 4, lines 1-67).

With respect to claim 34, O'Flaherty discloses, event service which allows an identity server to register interest in and be notified of changes in the database, see (col. 4, lines 1-67).

With respect to claim 35, O'Flaherty discloses, process to verify information gathered from a user registration form, see (col. 4, lines 1-67).

With respect to claim 36, O'Flaherty discloses, profile discovery and publishing service which allows users to publish at least a portion of their profile information, see (col. 4, lines 1-67).

With respect to claim 37, O'Flaherty discloses, allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 38, O'Flaherty discloses, form conversion service which assists a webmaster in converting existing forming to standardized field names, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 39, O'Flaherty discloses, install service which installs servlets on a web server, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 40, O'Flaherty discloses, identity exchange service for portions of a privacy protection protocol, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 41, O'Flaherty discloses, chat service which sets up chat rooms so users can communicate with each other in real time, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 42, O'Flaherty discloses,, presence service which lets users specify where they are and allows them to discover another user's presence information, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 43, O'Flaherty discloses, anonymous remailer service which allows users to choose different email addresses for different profiles, see (col. 9, lines 43-64).

With respect to claim 44, O'Flaherty discloses, anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information, see (col. 9, lines 15-23).

With respect to claim 45, O'Flaherty discloses, infomediary service which facilitates creating an infomediary, see (col. 9, lines 43-64).

With respect to claim 46, O'Flaherty discloses, tracking IP addresses in order to selectively publish the last known IP address of a user, see (col. 9, lines 43-64).

With respect to claim 47, O'Flaherty discloses, underlying directory service and an underlying file system in order to enforce access controls on web pages published by users, see (col. 9, lines 43-64).

With respect to claim 48, O'Flaherty discloses, email services, encodes contact relationship information in the user's email address, see (col. 9, lines 43-64).

With respect to claim 49, O'Flaherty discloses, contact relationship information in the user's email address, see (col. 9, lines 43-64).

With respect to claim 50, O'Flaherty discloses, profiles to filter email sent to the user, see (col. 9, lines 43-64).

With respect to claim 51, O'Flaherty discloses, determining whether a user logging in at a third party web site is registered as a user of the system, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 52, O'Flaherty discloses, logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 53, O'Flaherty discloses, registering the user and logging the user in comprises a means for capturing user login information for the third party web site, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 54, O'Flaherty discloses, user digital identity information is only made available to a partner site if the user has flagged the information as public, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 55, O'Flaherty discloses, icon provides a transaction history, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 56, O'Flaherty discloses, user authentication mechanism, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 57, O'Flaherty discloses, launch point for launching application, see (col. 8, lines 10-67 to col. 9, lines 1-64).

With respect to claim 58, O'Flaherty discloses, non-repudiation feature whereby an administrator cannot change a user password and then log on as the user, see (col. 7, lines 10-67 to col. 8, lines 1-61).

With respect to claim 90, O'Flaherty teaches, defining vault for a storage of one or more safes digital identities, (i.e., identity field includes security information (154 in fig. 2B, fig. 1) in fig. 2A-B, col. 7, lines 10-65), the vault including an access protocol layer (i.e., 150 in fig. 1, privacy service to control data access in fig. 1, col. 5, lines 29-63), an identity server layer (i.e., identity field in fig. 2A, col. 7, lines 10-65) and an identity manager layer (col. 4, lines 8-60) and having access right granted to one or more system administrators (i.e., by administrator for setting up data access and view, col. 8, lines 10-61) including management of the one or more safes of digital identities (i.e., identity field includes security information (154 in fig. 2B, fig. 1) in fig. 2A-B, col. 7, lines 10-65) of one or more accounts of end users (i.e., different data view for each user by each user's privilege in fig. 2A-C, col. 8, lines 10-67 to col. 9, lines 64), the one or more safes of digital identities having multiple profile (i.e., identity information in fig. 2A) each with access right granted exclusively to the end users via the one or more accounts (i.e., 154, security information provides in fig. 2A access control rule for each user, col. 5, lines 29-63, col. 10, lines 27-64) including the exclusion of access rights of the one or more system administrators, (by each user without system administrators, col. 8, lines 45-61), the multiple profiles (each user (not administrator) can change privacy preference, col. 8, lines 45-61) being shared amongst the end users at the exclusion of the one or more system administrators (i.e., identity information can be accessed and shared by anonymizing view for any user (not administrator) in fig. 2A, col. 7, lines 10-67 to col. 8, lines 1-67 to col. 9, lines 1-63).

With respect to claim 91, O'Flaherty teaches, one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP (col. 1, lines 28-67 to col. 2, lines 1-50).

With respect to claim 92, O'Flaherty teaches, the identity server layer serves as an NDS access point (col. 1, lines 28-67 to col. 2, lines 1-50).

With respect to claim 93, O'Flaherty teaches, identity server layer maintains access rights to the digital identities (154, in fig, 1, fig. 2B, col. 7, lines 11-67).

With respect to claim 94, O'Flaherty teaches, identity manager layer includes NDS authentication and authorization that controls access to the digital identities (in fig, 1, fig. 2B, col. 7, lines 11-67).

With respect to claim 95, O'Flaherty teaches, identity manager layer has a secret store (col. 7, lines 11-67).

With respect to claim 96, O'Flaherty teaches, the one or more processors and the one or more memories are located on an identity server (col. 6, lines 23-34).

With respect to claim 97, O'Flaherty teaches, the one or more processors and the one or more memories are functionally apportioned between a client, a web server and an identity server, including servlets and applets (col. 1, lines 27- to col. 2, lines 1-50).

With respect to claim 98, O'Flaherty teaches, vault for secure storage of one or more safes digital identities (i.e., identity field includes security information (154 in fig. 2B, fig. 1) in fig. 2A-B, col. 7, lines 10-65), the vault (i.e., database 104 in fig. 1) having an access protocol layer (i.e., 150, privacy service to control data access in fig. 1, col. 5, lines 29-63), an identity server layer (i.e., identity field in fig. 2A, col. 7, lines 10-65) and an identity manager layer (col. 4, lines 8-60) and having access right granted to one or more system administrators including management of the one or more safes of digital identities (i.e., different data view for each user by each user's privilege in fig. 2A-C, col. 8, lines 10-67 to col. 9, lines 64) the one or more safes of digital identities having multiple profile (i.e., identity information in fig. 2A) each with access right granted exclusively to the end users at location remote i.e., different data view for each user by each user's privilege in fig. 2A-C, col. 8, lines 10-67 to col. 9, lines 64) from the vault, including the exclusion of access rights of the one or more system administrators, (each user (not administrator) can change privacy preference, col. 8, lines 45-61), the multiple profiles (i.e., identity information in fig. 2A) being shared amongst the end users at the exclusion of the one or more system administrators (i.e., identity information can be accessed and shared by anonymizing view for any user (not administrator) in fig. 2A, col. 7, lines 10-67 to col. 8, lines 1-67 to col. 9, lines 1-63).

With respect to claim 99, O'Flaherty teaches, identity manager layer (identity field includes security information (154 in fig. 2B, fig. 1) in fig. 2A-B, col. 7, lines 10-65), client interface (i.e., client in fig. 1, col. 4, lines 1-67).

With respect to claim 100, O'Flaherty teaches, client application interface, see (i.e., client in fig. 1, col. 4, lines 1-67).

With respect to claim 101, O'Flaherty teaches, the safe object containing at least one profile of the digital identity profiles administered by a user, see (col. 8, lines 46-61).

(10) Response to Argument

Applicant argued:

The prior art, reference O'Flaherty et al (U.S. Patent No. 6,275,824, hereinafter, "O'Flaherty") does not teach, "different profiles administered exclusively by a single one of the multiple users at the exclusion of the system administrator" and "access protocol layer, identity server layer and identity manager layer".

However, examiner disagrees.

Ⓐ First ~~Fist~~ of all, the claimed limitation includes a logical discrepancy itself regarding administrator. Claims (1, 90 and 98) recite, "access right ***granted to a system administrator*** for management of the multiple user object" (on lines 4-5 for claim 1 and on lines 5-6 for 90 and on lines 4-5 for 98). However, claims (1, 90 and 98) also recite, "accessed ..... ***at the exclusion of the system administrator***" (on lines 6-7 for claim 1 and on lines 7-9 for 90 and on lines 5-7 for 98), which does not make sense. Because access right is granted to a system administrator and also access right is excluded to a system administrator. Thus, it fails to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Examiner interprets the claim limitations as argued by applicant above as, "administered (accessed) only by a single user without the system administrator's right". So only authorized a single user who has no administrator right can accesses (administrates) the profiles. O'Flaherty discloses, "the standard view 260 selectively masks personal data from view unless the consumer has had the appropriate flags set to the proper value (col. 8, lines 16-24)" and "dataviews are established using the same names that are used for base tables in any existing applications that access private data, and corresponding base table names can be renamed to some other value. Thus, whenever an existing application attempts to access private data (now via a dataview), the private data can be screened out by the dataview, depending on user privileges" (col.8, lies lines 35-42) and "the client interface module 212, which is used to view, specify, and change consumer privacy preferences, is a privileged application. Appropriate security measures are undertaken to assure that the privileged applications are suitably identified as such, and to prevent privileged view 262 access by any entity that is not so authorized" (col. 8, lines 46-61). This teaches that only a single user (who has not administrator right) can access (administer) his or her own privacy preferences (profiles), with exclusion of accessing by unauthorized user. Thus, only authorized user without administrator's right can access the profiles. Therefore, O'Flaherty teaches, "different profiles administered exclusively by a single one of the multiple users at the exclusion of the system administrator". And "access protocol layer, identity server layer and identity manager layer" that are all computer software program instructions to perform the claimed limitation in a computer system. Each software function layer does not have any specific invention step or weight unless further defines. In any way, O'Flaherty teaches privacy service to control data accessing (150 in fig. 2A-B, col. 5, lines 29-63, col. 7, lines 10-65, access protocol layer), server (col. 5, lines 13-16, identity server layer) and administrator rolls (col. 8, lines 10-

61, identity manager layer). Therefore, O'Flaherty teaches, "different profiles administered exclusively by a single one of the multiple users at the exclusion of the system administrator" and "access protocol layer, identity server layer and identity manager layer".

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Isaac Woo
July 30, 2007 Isaac Woo

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER

Conferees:

	Hosain Alam	AU: 2166 SPE
FW	Tim Vo	AU: 2168 SPE

Mohammad Ali
SPE, 2169